클라우드 도입

오늘날, 미래의 SOC를 계획하는 방법

AI 및 자동화 기반의 보안 운영 혁신을 위한 종합 플레이북

목차

그 어느 때보다 어려운 SOC의 당면 과제

보안 위협은 보안 기술보다 훨씬 빠른 속도로 진화하고 있으며, 자금이 든든한 공격자는 머신 러닝(ML), 자동화, 인공 지능(AI) 등의 도구에 투자를 아끼지 않고 있습니다. 현재 운영되고 있는 클라우드 네이티브 애플리케이션이 7억 5천만 개를 넘어선 가운데,[1] 지난 1년간 클라우드 표적 공격이 66% 증가[2]하는 등 클라우드 환경의 문제는 특히 심각합니다. 기존 보안 정보 및 이벤트 관리(SIEM)를 중심으로 구축된 SOC는 정확한 탐지를 목적으로 설계되지 않았으며, 특히 공격자가 취약점을 악용하고, 내부망 이동을 감행하며, 대량의 데이터를 유출할 수 있는 동적 클라우드 환경을 고려하여 구축되지 않았습니다. 따라서 디지털 혁신, 클라우드 이니셔티브, 지능형 공격과 속도를 맞출 수 있는 탐지 엔지니어링을 위해 ML을 활용하는 데는 그다지 효과가 뛰어나지 않습니다.

기존 SOC 환경의 문제점을 예로 들면 다음과 같습니다.

- 클라우드 워크로드, 제어 플레인, 구성 전반의 가시성 및 컨텍스트 부족
- 전체 공격을 파악하기 위해 여러 이벤트의 상호 연관성을 수동으로 구성하는 등 조사 복잡성 증가
- 클라우드 및 전통적 환경 전반에 걸친 위협 인텔리전스 데이터의 수집, 처리, 컨텍스트화 역량 부족
- 퍼블릭 및 프라이빗 클라우드 환경 전반에 걸쳐 충실도가 낮은 대량 알림이 발생함에 따른 알림 피로 및 노이즈
- 클라우드 대상 인시던트 대응을 위한 자동화 및 오케스트레이션 부족
- SOC가 클라우드 팀과 분리되어 있는 경우가 많으며, 클라우드 워크로드에 대한 런타임 보호 기능 부족
- 클라우드 환경의 컨테이너 이스케이프, 내부망 이동, 권한 상승에 적절하게 대응하지 못하는 실시간 보호 기능

이러한 문제는 통합 보안 플랫폼 접근 방식의 필요성을 강조합니다. 더 이상 클라우드 보안과 SOC 운영을 분리하여 관리해서는 안 됩니다. 클라우드 워크로드 보호, 위협 탐지 및 대응, 자동화, AI 기반 분석을 모두 결합한 통합 플랫폼은 사일로형 구조를 제거하고, 정교한 최신 공격에 대응하기 위해 필요한 포괄적 가시성과 제어 기능을 제공하며, 운영 효율성을 향상합니다.

1. "The future of application delivery starts with modernization," IBM Security, 2024년 4월 10일.
2. *Unit 42 인시던트 대응 보고서*, Palo Alto Networks, 2024년 2월 20일.

필수 요소가 된 SOC 플랫폼화

사이버 공격이 더욱 가속화되고 정교해지면서, 공격자의 역량과 기존의 단편적 보안 접근 방식 간에 심각한 격차가 발생하고 있습니다. 이로 인해 플랫폼화는 현대 보안 운영 센터에서 반드시 필요한 요소로 자리 잡고 있습니다. 여러 공급업체의 보안 도구를 조합하여 사용하는 경우 도구마다 상이한 관리 환경과 데이터 사일로가 형성되며, 이는 조직이 위협을 신속하게 탐지하고 대응하는 데 방해가 됩니다. 플랫폼화는 공통 데이터와 관리 체계를 기반으로 보안 기능을 단일 플랫폼으로 통합함으로써 이러한 문제를 해결합니다. 또한, AI 기반 자동화를 지원하여 대응 시간을 몇 시간 단위로 크게 단축하고, 포인트 솔루션으로 인해 발생하는 복잡성과 보안의 공백을 해소할 수 있습니다.

플랫폼 접근 방식은 다음과 같은 기능을 통해 보안 운영을 혁신합니다.

통합 가시성 및 제어

포괄적 데이터, AI, 자동화를 기반으로 하는 통합 플랫폼은 다음과 같은 이점을 제공합니다.

- **선제적 애플리케이션 보안**: 컨텍스트 인식 가드레일은 개발 과정 전반에 걸쳐 취약점을 식별하고 우선순위를 지정하여 코드가 프로덕션 단계에 도달하기 전에 리스크를 감소시킵니다.
- **AI 기반 런타임 예방**: Cortex XDR® 에이전트와 같은 도구는 탁월한 런타임 보호 기능을 제공하며, MITRE ATT&CK 테스트에서 완벽한 효율성을 증명했습니다.
- **클라우드 탐지 및 대응(CDR)**: AI 기반의 우선순위 지정 및 조사 기능은 공격을 신속하게 감지하고 완화시켜 기업 전반의 문제 해결 프로세스를 자동화합니다.
- **DevSecOps 간소화**: 통합 자동화 기능은 수동 워크플로를 제거하고 코드, 클라우드 태세, 런타임 환경 전반에 걸친 수정을 지원합니다.
- **생성형 AI 기반 생산성**: GenAI 코파일럿은 워크플로를 가속화하여 팀 간 협업과 효율성을 향상시킵니다.

대규모 운영 효율성

- 통합 플랫폼은 측정 가능한 여러 운영상 이점을 제공합니다.
- 알림의 90%가 자동 해결되므로 수동 워크로드가 크게 감소했습니다.
- 신속한 위협 탐지 및 대응: MTTD에 10초, MTTR(응답)에 1분이 소요됩니다.
- MTTR(해결) 5시간으로 인시던트를 효율적으로 관리합니다.
- 통합 플랫폼에서 운영되므로 트레이닝 비용이 크게 절감됐습니다.

비즈니스 가속화

가장 중요한 것은, 통합 플랫폼은 리스크를 감소시키면서도 더 빠르게 움직일 수 있도록 지원한다는 점입니다.

- 포괄적 가시성과 내장된 보안 기능을 통해 새로운 클라우드 서비스의 배포에 소요되는 시간을 단축합니다.
- 도구를 통합하고 운영 복잡성을 줄여 총 소유 비용을 절감합니다.
- 애플리케이션, 클라우드, 보안팀 전반의 생산성을 향상시켜 대규모의 보안 혁신을 지원합니다.

미래 지향적 SOC를 위한 5단계

1단계: 수동 SOC 모델 혁신

수동 SOC 모델은 온프레미스 소프트웨어 형태로든 클라우드로 제공되든, 인간 애널리스트가 중심입니다. SOC 애널리스트는 하루에 수백 개의 알림을 살펴보며 컨텍스트 데이터를 수집하여 수동으로 분류하고, 대부분의 시간을 오탐과 수작업을 처리하는 데 보냅니다. 그러나 알림 양이 많아지고 시스템이 많아지면서 데이터를 통합하기 어려워진 탓에, 인간 중심의 접근 방식이 힘들어졌습니다. 대신, 효과적으로 SOC를 확장하는 현대적인 방법으로 자동화를 기반으로 애널리스트가 소량의 고위험 인시던트를 처리하는 방식이 대두되었습니다

상용 항공기를 조종할 때 조종사가 계속 직접 제어할 필요가 없듯, 자동화 중심 SOC도 위험도가 낮고 반복되는 알림, 분석 작업, 완화 같은 작업을 대부분 직접 처리합니다. 이렇게 하면 애널리스트가 긴급하고 영향이 큰 인시던트를 처리할 수 있고, 기본 플랫폼은 '자동 조종' 방식으로 SOC를 이용해 안전한 결과를 냅니다. 각각의 활동에서 학습해 '기장'에게 정보와 효과적인 권장 사항을 제안하는 것입니다. 바로 이것이 Palo Alto Networks의 자율 SOC 비전입니다.

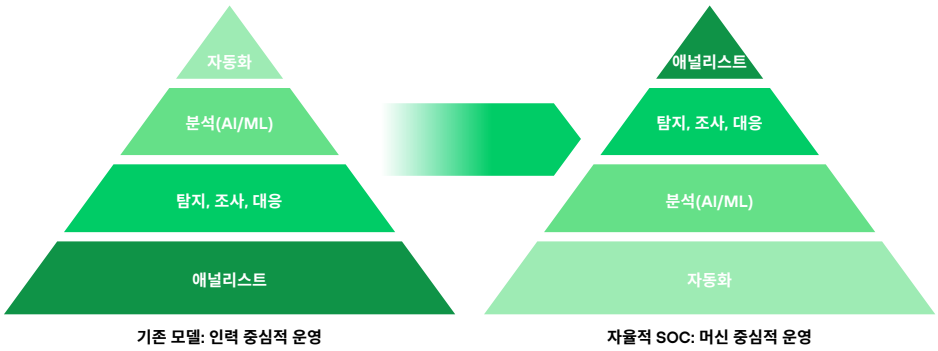

그림 1: 인력 중심 운영과 시스템 중심 운영 비교

궁극적으로, 데이터 모델링과 통합을 개선하고 여기에 자동 분석과 탐지를 함께 활용하면 보안 엔지니어의 부담을 덜 수 있습니다. 엔지니어가 데이터를 통합하고 위협을 탐지하기 위해 맞춤 상관관계 규칙을 구성할 필요가 없어지기 때문입니다. 최신 SOC는 레거시 보안 운영과 달리 사람의 판단력에 의존하거나 이미 지나간 위협을 잡는 데 급급한 규칙에 의존하지 않고, 대량의 데이터 세트에 데이터 사이언스를 적용하는 것이 핵심입니다.

최신 SOC는 새로운 아키텍처, 데이터 활용법, 프로세스를 활용해 최신 위협을 해결하기 위해 전과는 다른 접근 방식으로 구축하고, 다음과 같은 위협 현황에 대한 지식을 지속적으로 업데이트해야 합니다.

- 광범위한 자동 데이터 통합, 분석 및 분류
- 애널리스트의 생산성을 지원하는 통합 워크플로
- 최소한의 애널리스트 지원으로 공격을 차단할 수 있는 내장형 인텔리전스 및 자동 대응

2단계: 환경을 감사하면 도구 확산의 보안 리스크 완화 가능

레오나르도 다빈치는 "단순함이 가장 정교한 것"이라는 말을 남겼습니다. 수많은 기업이 인수합병을 거치고 비슷한 보안 제품 여러 개를 정규화하지 못해 보안 스택 전체에 이질적인 도구가 넘쳐나는 곤란을 겪고 있습니다. 간단히 말해, 도구가 너무 많으면 그만큼 문제도 많이 생깁니다. 또한 리소스가 클라우드 환경과 온프레미스 인프라에 흩어져 있으므로 공격 표면을 완벽하게 파악하기 어렵습니다. 효과적인 보안 태세는 명확한 인벤토리화에서 시작됩니다. 어떤 클라우드 제공업체가 연결되어 있는지, 각 CSP는 어떤 서비스를 활용하는지, 온프레미스 환경에 액세스 가능한 자산은 무엇인지 등을 파악해야 합니다. 이러한 기초적 이해 없이는 실제 공격 표면을 효과적으로 파악할 수 없습니다.

팀에 따라서는 특정 문제를 해결하기 위해 포인트 솔루션을 배포한 것을 계기로 툴이 확산되기 시작되기도 합니다. 안타깝게도 이렇게 단편적인 접근 방식을 취하고 수많은 에이전트를 관리하다 보면 (역설적이게도) 네트워크가 더 취약해질 수 있습니다. 상호운용성이 결여되고 다양한 솔루션 전체에 부적절한 구성이 존재하다 보니 빈틈이 드러나게 됩니다.

도구 확산으로 인한 보안 저하를 줄이기 위한 첫 단계는 보호되는 시스템과 엔터티를 대상으로 감사를 실시하는 것입니다.

정확히 무엇이 보호되고 있고, 무엇을 방지하고 있는지 확실히 파악해야 합니다. 지적 재산일 수도 있고, 고객의 개인정보일 수도 있습니다. 소프트웨어든 물리적 자산이든 최대한 정보를 많이 파악할수록 고가치, 고위험 데이터를 보호하기 위해 우선순위를 정하는 데 도움이 됩니다.

일단 보호 대상이 무엇인지 명확하게 파악하고 나면, 논리적인 다음 단계는 여러 가지 요구 사항을 해결할 수 있는 솔루션을 찾는 것입니다. 2022년에 ESG(Enterprise Strategy Group)가 IT 및 사이버 보안 전문가 280명(미국, 캐나다, 유럽, 중남미, 아프리카, 아시아, 호주)을 대상으로 실시한 설문조사에 따르면 전체의 22%는 사이버 보안을 목적으로 구매한 단절된 포인트 제품이 너무 많아 이를 관리하기 복잡해서 힘들다고 답했고, 응답자 중 66%는 사용 중인 보안 제품이 25개 이하라고 밝혔습니다.[3] 현재 상황에서는 다양한 도구에 센서와 보강 요소를 일일이 갖출 필요가 없으므로, 가능하면 최대한 통합을 추구하는 것이 좋습니다.

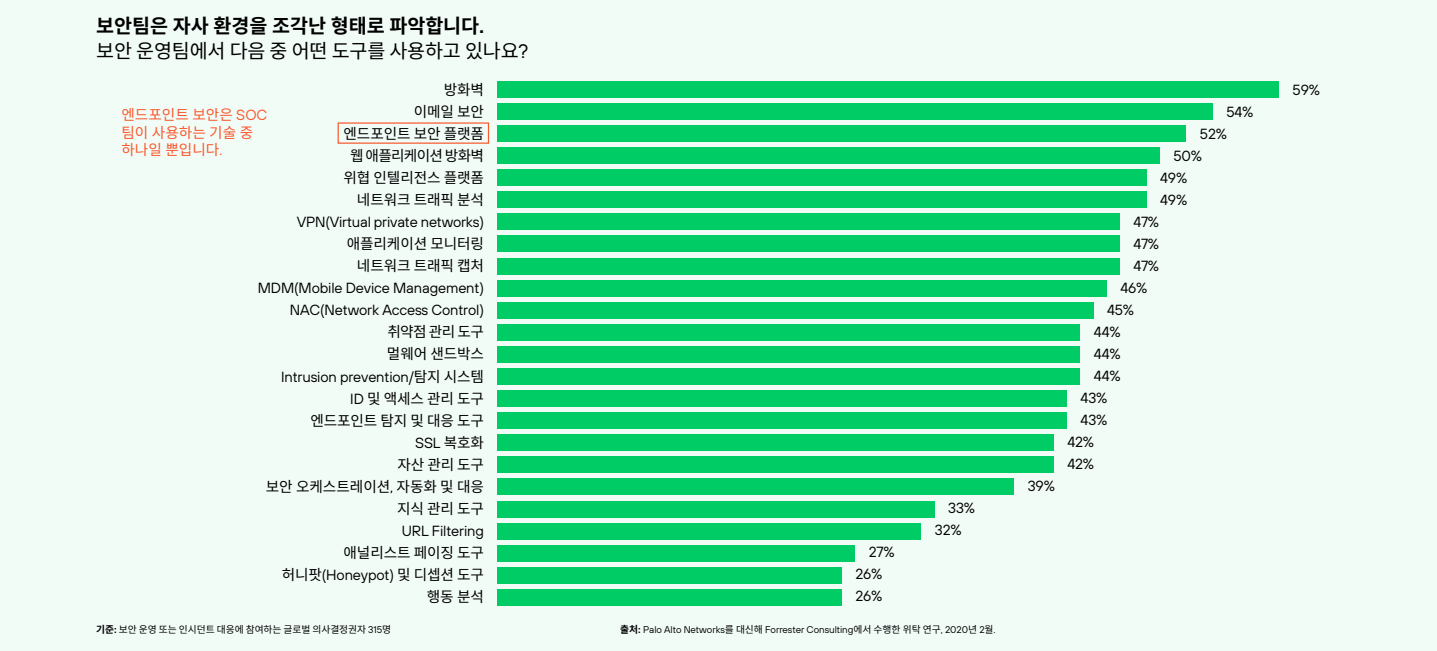

그림 2: 보안 운영의 프로가 사용하는 도구, Forrester에 직접 보고[4]

3단계: 워크플로 자동화

보안 리더는 도구를 선정할 때 구성이나 가동에 인간의 개입이 꼭 필요한지 고려해야 합니다. 결과를 해석하거나 분류할 때 반드시 전문가가 개입해야 하는가? 사용자의 테스트가 필요한가? 보안 리더가 반복 가능하고 수준이 낮은, 사람의 의사결정이 필요한 작업을 파악해두면 인시던트 조사 속도를 높일 수 있습니다. 머신 러닝과 인공 지능의 발전은 장래성이 매우 크기는 하지만 원활한 SOC 혁신에서는 어느 방향으로든 지식 이전에 인간적 요소를 유지하는 것이 최적의 결과를 얻는 데 매우 중요합니다.

모니터링해야 할 수많은 위협 피드를 비롯하여 보안 운영과 인시던트 대응(IR)에 수동 프로세스가 너무 많으므로 보안 오케스트레이션, 자동화 및 대응(SOAR) 솔루션과 같은 자동화 기능에 투자하면 제품 스택에서 오케스트레이션 작업을 촉진하고 더욱 빠르고 확장 가능한 IR을 실현할 수 있습니다.

3. *Cybersecurity Process and Technology Survey*, ESG, 2022년 6월.
4. *보안 운영 현황*, Palo Alto Networks에서 의뢰한 Forrester Consulting 연구, 2020년 2월.

자동화를 통해 SOC(및 클라우드)의 편의성을 향상하는 방법

- **인시던트 대응 가속화**: 수동 작업을 자동화하여 응답 시간을 단축하고, 컨테이너 이스케이프 및 권한 상승 시도 등 기존의 위협과 클라우드 위협에 대한 탐지 정확도를 모두 향상시킵니다.
- **프로세스 표준화**: 복제 가능한 워크플로를 구현하여 인시던트 대응 프로세스를 표준화하고, 일상적인 클라우드 구성 점검 및 규정 준수 모니터링을 자동화합니다.
- **보안 운영 통합**: 다양한 보안 제품과 클라우드 도구 전반에 걸쳐 워크플로를 오케스트레이션함으로써 통합적 인시던트 대응을 지원합니다.
- **생산성 향상**: 클라우드 및 기존 보안 이벤트의 자동 상관관계 분석을 통해 애널리스트가 반복 작업에서 벗어나 전략적 업무에 집중할 수 있도록 돕습니다.
- **투자 효과 극대화**: 자동화를 통해 여러 보안 제품을 효율적으로 조율하고, 기존 보안 도구의 활용 가치를 극대화합니다.
- **인시던트 처리 간소화**: 주요 ITSM 플랫폼 및 커뮤니케이션 도구의 티켓 관리와 이해관계자 알림을 자동화하여 해결 속도를 향상합니다.
- **클라우드 보안 강화**: 지속적 모니터링과 자동 위협 대응을 지원하며, 클라우드 팀과 SOC 팀 간의 협업을 간소화합니다.
- **전반적 태세 개선**: 클라우드 및 전통적 환경을 포괄적으로 자동화하여 보안 및 비즈니스 리스크를 줄입니다.
- **팀 협업 지원**: SOC, CloudSecOps, DevOps 팀 간의 인시던트 라우팅을 자동화하고, 통합 협업 도구와 자동 인시던트 후속 조치 및 추적을 통해 실시간 커뮤니케이션을 지원하며 대응을 조율합니다.

4단계: ML 기반 인텔리전스로 인력 보강

최신 SOC 혁신의 핵심 요소는 보안팀이 머신 러닝과 인공 지능을 모두 활용해 보안 업무를 처리하는 사람의 역량을 증강하고 보완하는 것입니다. ML과 AI를 활용하면 대량의 데이터를 처리해 중요한 보안 인사이트를 개발하는 데 드는 시간을 대폭 단축할 수 있습니다. 여러 데이터 소스에서 이상 패턴을 탐지하고, 컨텍스트가 포함된 알림을 자동으로 제공하는 현대의 ML 및 AI는 조사 속도를 단축하고 엔터프라이즈에서 사각지대를 제거할 수 있습니다.

이 경우 ML 모델을 훈련하고, 이를 사용하여 데이터 사이에서 패턴을 탐지한 다음, 프로세스를 테스트하여 개선하는 방식으로 운영됩니다. ML 및 AI 기법은 데이터를 수집, 통합, 분석하여 정보를 얻고 인간이 이러한 작업을 수행하는 데 필요한 시간과 지식을 줄여줍니다. 또한 이렇게 하면 SOC 팀이 데이터에 포함된 여러 보안 계층에서 위협 컨텍스트와 증거를 찾고자 하는 SOC 팀의 문제를 최소화합니다.

ML 기법을 사용하면 데스크톱 컴퓨터, 메일 서버나 파일 서버와 같은 디바이스에서 디지털 마커를 읽고 여러 가지 디바이스 유형의 행동을 학습해 이상 동작을 탐지할 수 있습니다. 예를 들어, ML 모델은 다양한 차원에서 애플리케이션의 정상 패턴을 학습함으로써 환경 내부 애플리케이션의 행동 기준을 설정합니다.

- 파일 시스템 상호 작용(일반적으로 액세스하는 파일 및 디렉토리)
- 프로세스 동작(예상되는 상위/하위 관계, 프로세스 트리 구조)
- 네트워크 통신(일반 연결 패턴, 프로토콜, 대상)
- 리소스 사용(표준 CPU, 메모리, I/O 패턴)

ML 모델이 애플리케이션이 미승인 파일에 액세스하거나, 비정상적 프로세스를 생성하거나, 일반적이지 않은 네트워크 연결을 설정하는 등 이상 동작을 탐지할 경우 잠재적인 보안 인시던트 알림을 트리거할 수 있습니다. 이러한 접근 방식은 공격자가 정상 애플리케이션을 악용하는 리빙 오프 더 랜드(Living off the land) 공격을 식별하는 데 특히 효과적입니다.

Palo Alto Networks의 Precision AI®는 통합 시스템에 다양한 AI 접근 방식을 결합하여 이 기능을 더욱 발전시킵니다. 머신 러닝을 활용하여 정확한 방어 및 예측을 구현하고, 딥 러닝을 활용하여 실시간 예측 모델을 구축하며, 생성형 AI를 활용하여 사람이 읽을 수 있는 인사이트를 제공함으로써 사용자 경험을 간소화합니다. 이러한 독자적 시스템은 풍부한 데이터와 보안 전용 모델을 사용하여 탁월한 정확도로 탐지, 예방, 수정을 자동화하고 오탐을 축소함으로써 보안팀에게 신뢰할 수 있는 AI 결과를 제공합니다.

요약하자면, ML 및 AI 기법은 다음과 같은 기능을 제공합니다.

- **통합**: 데이터가 현재 상황에 대해 전달하도록 지원
- **분석**: 문제 영역에 대한 인사이트를 추출하고 예측
- **자동화**: 사람의 의사결정 속도를 높이고 시스템 레벨 작업, 워크플로, 의사결정 자동화
- **학습**: 지속적으로 신종 위협과 공격 패턴에 맞춰 조정
- **향상**: 인적 전문성을 강화하여 보안 성과 개선

5단계: 보안팀 최적화

보안 솔루션과 도구에 투자하는 수준 이상으로 SOC 성공을 좌우하는 중요한 요소는 지금도 변함없이 인적 요소입니다. 머신 러닝과 자동화가 대응 시간, 정확도, 전반적인 복구 업데이트 성과를 개선해주는 것은 분명한 사실이지만(특히 난이도 수준이 낮은, 반복적인 작업의 경우), 일관성 있는 SOC 혁신 전략이라면 반드시 엔지니어, 애널리스트, 아키텍트 등 보안 직원의 유치, 교육, 유지를 기본적으로 포함해야 합니다. 기업에서는 자동화 기술을 활용해 비즈니스 보호 효율을 강화할 수 있습니다.

미국 노동 통계국에 따르면 2019년부터 2029년까지 사이버 보안 업종에 종사하는 인원수가 31% 늘어날 것으로 전망된다고 합니다.[5] 또한 미국 국립 교육 통계 센터(NCES)에서는 지난 6년간 신규 사이버 보안 프로그램 수가 33% 늘어나고, 사이버 보안 부문의 채용 공고는 94%나 늘어났다고 밝혔습니다.[6]

중요한 직무에 인력을 충원하는 것도 물론 중요하지만, 직원, 하청업체, 파트너(경우에 따라)에게 사이버 보안 인식 교육을 제공해 침해 예방을 돕는 데 필요한 실력을 갖추게 하는 것도 그만큼 중요합니다. 자격 증명 도용, 피싱 공격, 소셜 엔지니어링 등은 캠페인을 실행할 사람이 필요하므로, 사이버 노하우를 갖춘 팀을 구축하는 것은 장기적으로 가치 있는 일입니다. 유명 암호 해독가이자 컴퓨터 보안 전문가인 Bruce Schneier는 "보안에서 가장 취약한 부분은 사람일 때가 많고, 보안 시스템 오류의 고질적인 원인도 사람"이라고 했습니다.

Cortex: SOC 혁신의 기반

회복력이 우수하고 효과적인 SOC를 구축하기 위한 기본 토대는 위와 같은 다섯 가지 단계를 밟는 것부터 시작합니다. 그리고 다음과 같은 다섯 가지 기술 "요점"을 고려해 보안 운영 전략을 수립해야 합니다.

요점 1: 공격 표면을 파악해 리스크 관리 지원

SOC 혁신의 기본적 구성 요소는 강력한 리스크 관리 기능입니다. 리스크 관리 프로세스의 첫 단계는 당연히, 공격을 방지하고 보호하고자 하는 대상을 확인하는 것입니다. 이를 통해 리스크 관리 계획이나 전략(기본적인 형태든, 강화된 버전이든)의 컨텍스트를 정립합니다. 이런 확인부터 시작하면 무엇이 위험한지 우선순위를 정하고, 각 리스크를 완화하려면 무엇이 필요한지 분석할 수 있습니다.

5. *Occupational Outlook Handbook, Information Security Analysts*, U.S. Bureau of Labor Statistics, 2021년 4월 9일.
6. *CISO Benchmark Study*, Cisco, 2019년 3월.

리스크 관리 기능에 도움이 되는 중요한 단계로는 공격 표면을 명확히 이해하는 것이 있습니다. 볼 수 없으면 보호할 수도 없습니다.

조직의 **공격 표면**을 구성하는 요소. . .

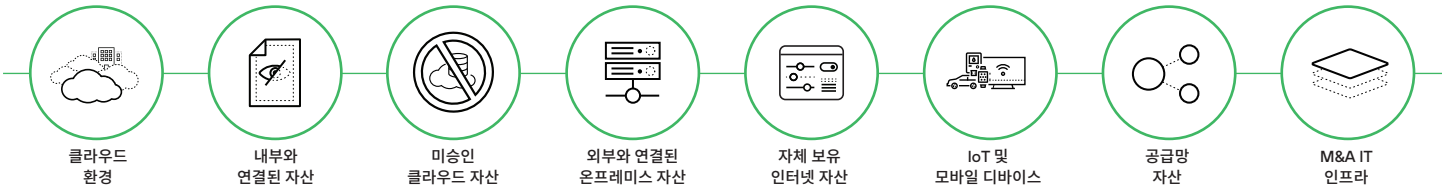

그림 3: 공격 표면의 구성 요소

그러나 공격 표면 관리(ASM) 솔루션을 구축하거나, 침투 테스트, 취약점 스캔 등의 선제적 평가를 실행하더라도 제품과 운영 요구 사항을 모두 알아내야 가장 알맞은 사용 사례를 찾을 수 있습니다. 제품과 운영 요구 사항에는 기능, 특징, 역량, 평가 기준이 포함되며, 이는 ASM 솔루션이나 도구에서 기대할 만한 특징과 기능을 요약하는 데 도움이 됩니다.

*Cortex Xpanse 공격 표면 위협 보고서*에는 세계적인 몇몇 대기업의 공개 인터넷 공격 표면을 대상으로 Palo Alto Networks가 실시한 리서치를 통해 알아낸 조사 결과가 기재되어 있습니다. 1월부터 3월까지, Cortex Xpanse® 연구팀은 범죄자들이 빠른 익스플로잇을 위해 취약한 시스템을 얼마나 신속하게 식별하는지 알아보기 위해 글로벌 기업 50사와 관련된 5,000만 개의 IP 주소 스캔을 모니터링했습니다.

흥미롭게도, 발견된 취약점 3개 중 1개 정도가 RDP(Remote Desktop Protocol) 문제에 기인한 것으로 밝혀졌습니다.[7] RDP는 기업이 COVID-19 팬데믹으로 인해 새로운 재택근무(WFH) 프로토콜에 영향을 받은 원격 근무자를 지원하기 위해 2020년대 초부터 클라우드로의 이동에 박차를 가하면서 사용이 급증했습니다. 이외에 다음과 같은 조사 결과가 나왔습니다.

- **공격자는 끊임없이 공격을 시도합니다.** 공격자는 마치 절대로 끝나지 않는 "꼬리잡기"를 하듯 매시간 새로운 스캔을 시도하지만, 글로벌 기업에서는 몇 주에 걸쳐 한 번씩 스캔합니다.[8]
- **공격자는 새로운 취약점에 즉시 반응합니다.** 공격자는 1월부터 3월 사이에 새로운 CVE(Common Vulnerabilities and Exposures)가 발표되자마자 15분 내로 스캔을 시작하고, Microsoft Exchange Server 제로데이 보안 업데이트가 출시되자마자 5분 내로 스캔을 개시했습니다.[9]
- **취약한 시스템은 무수히 많습니다.** 전 세계 기업에서 심각한 노출이 새로 발견되는 간격은 평균 12시간에 한 번, 즉 하루에 두 번입니다. 여기에는 취약한 원격 액세스(RDP, Telnet, SNMP, VNC 등), 데이터베이스 서버, Microsoft Exchange Server 및 F5 로드 밸런서와 같은 제품의 제로데이 취약점 노출 등이 포함됩니다.[10]
- **클라우드 침해는 보안팀의 가장 큰 걱정거리입니다.** 글로벌 엔터프라이즈에서 발견되는 가장 치명적 보안 문제에서 클라우드 비중은 79%를 차지하며, 클라우드 호스팅/기반 서비스의 리스크를 그대로 답습합니다. 반면, 온프레미스의 비중은 21%에 불과합니다.[11]

요점 정리: 스캔 기술이 발달하면서 공격자가 공격 벡터 위치를 빠르고 손쉽게 찾아낼 수 있게 되었습니다. 공격자는 버려지거나 잘못 구성된 무단 자산의 존재를 드러내 침해를 위한 백도어로 이용합니다. 공격 표면 관리 솔루션을 구축하면 기업의 외부 공격 표면에 연속적인 평가를 제공할 수 있습니다.

7. *2021년 Cortex Xpanse 공격 표면 위협 보고서*, Palo Alto Networks, 2021년 5월.
8. 출처 동일
9. 출처 동일
10. 출처 동일
11. 출처 동일

요점 2: SOAR - 제품 스택 전체를 오케스트레이션하여 효율적인 인시던트 대응 보장

SOAR의 경우, 자동 대응 워크플로를 설명하는 플레이북을 실행하는 솔루션이 떠오를 수 있지만 효과적인 SOAR 전략은 단순히 자동화를 활용하여 수동 작업을 간소화하고 제거하는 데 그치지 않습니다. 워크플로는 여러 가지 다른 기술과 통합하여 오케스트레이션하면 되고, 자동화를 통해 다음과 같이 바람직한 결과를 얻을 수 있습니다.

- 인시던트 알림 분류
- 위협 선별
- 인시던트 대응
- 위협 인텔리전스 구성 및 관리
- 규정 준수 모니터링 및 관리

SAN 보안 운영 자동화 현황 조사에 따르면, 자동화를 가장 많이 진행하는 대상은 피싱, 취약성 대응, 데이터 보강이며, 대부분의 응답자는 자동화를 통해 인시던트 대응의 50~75%를 처리하는 것을 목표로 삼고 있습니다.[12] 모든 측면의 인시던트 관리를 해결하는 포괄적 SOAR 솔루션은 SOC에서 일반적으로 사용하는 도구, 워크플로 자동화에 도움이 되는 모범 사례 플레이북, 통합 사례 관리 및 실시간 협업을 포괄적으로 기본 통합하여 팀 간 인시던트 조사를 지원해야 합니다.

마지막으로 (내부 및 외부) 위협 인텔리전스에 중앙 리포지토리 역할을 하는 기능은 지표, 인시던트, 인텔리전스의 상관관계를 자동으로 발견함으로써 보안 애널리스트와 인시던트 대응 담당자가 자세한 전략적 인텔리전스를 얻고 위협 행위자와 공격 기술에 대한 추가적 인사이트를 확보할 수 있어야 합니다.

SOAR 솔루션은 최신 SOC 환경의 제어 플레인이 되도록 구축되는 추세이고, 앞으로는 여러 가지 보안 운영 기능의 제어 플레인이 될 가능성이 있습니다. SOAR 플랫폼은 이 목표를 달성하기 위해 위협 인텔리전스, 취약점 관리, 클라우드 보안, 네트워크 보안 등을 플랫폼에 직접 통합하고 자동화를 SOC 이외의 사용 사례에도 확대 적용하고 있습니다. 또한, 주요 보안 공급업체는 특정 기술에 맞게 사전 프로그래밍되고 최적화된 자사 제품에 SOAR 및 인시던트 관리 기능을 포함하고 있습니다.

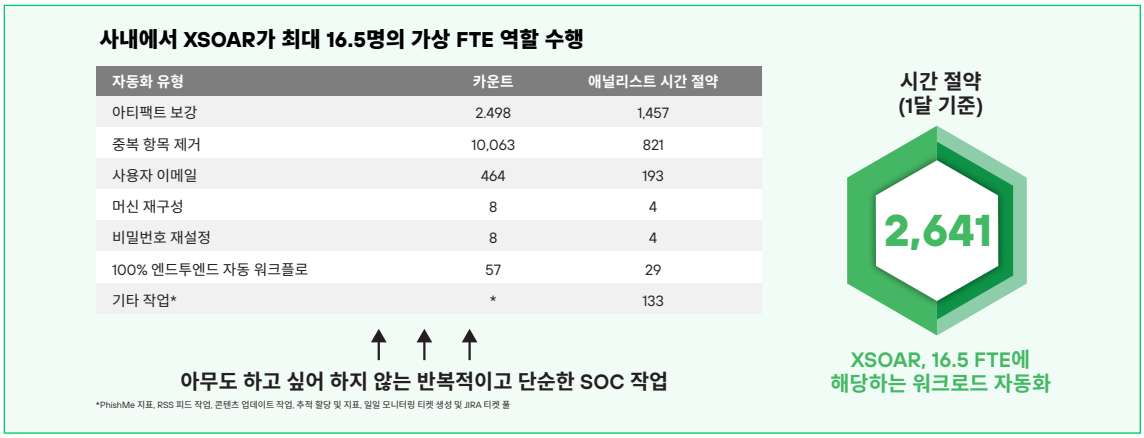

그림 4: 자동화를 통한 시간 절약 주요 사례

요점 정리: SOAR 솔루션의 핵심은 최소한의 인력 개입이 필요한 보안 이벤트에 대해 우선순위를 설정하고 간소화된 워크플로를 구축하는 기능입니다. SOAR 플랫폼은 프로세스를 자동화하고 SOC 제품 스택 전체에서 복잡한 인시던트 조사, 오케스트레이션을 최소화하는 단 하나의 플랫폼 역할을 하여 효율성이 개선됩니다.

12. Mark Orlando, *The State of Automation in Security Operation: A SANS Survey*, SANS Institute, 2024년 6월 13일.

요점 3: 탐지와 대응의 공백을 메워주는 XDR

"XDR"은 "Extended Detection and Response(확장형 탐지 및 대응)"의 줄임말로 2018년에 Palo Alto Networks의 CTO 겸 공동 창립자인 Nir Zuk가 처음으로 언급했습니다. XDR이 탄생한 근본적인 이유는 더욱 효율적으로 공격을 차단하고, 예방할 수 없는 공격자 기술과 전략을 탐지하고, SOC 팀이 조사가 필요한 위협에 더욱 잘 대응하는 데 도움이 되기 때문입니다. 이 접근 방식은 EDR, 네트워크 방화벽, ID 제공자, 클라우드 인프라, 그리고 기타 확장된 소스를 포함한 다양한 데이터 소스에서(경우에 따라 상호 보완적 데이터 소스) 분산된 원격 분석 정보를 가져와 공격의 컨텍스트를 강화하는 것입니다.

XDR을 사용하면 사일로화된 도구를 통합하고 프로세스를 간소화하며 위협 탐지 및 조사를 위한 가시성을 강화해 보안팀이 더 효율적이고 효과적으로 공격을 차단하는 데 도움이 됩니다. 또한 팀원들의 사각지대를 없애고 조사 시간을 단축하며, 궁극적으로 보안 성과를 개선할 수 있습니다. XDR의 기능으로 지속적 공격 기술이 광범위한 횡적 피해를 주기 전에 중요한 단계(예: 실행)에서 공격 시퀀스를 차단하면 보안팀에서는 '공격을 중간에서 저지하는' 솔루션을 갖출 수 있습니다.

XDR 도입을 뒷받침하는 요인으로는 엔드포인트 보안 혁신, 공격 주기 전반적으로 복잡한 공격의 단순한 시각화, 대응 자동화, 지능형 분석, 머신 러닝 기반 위협 탐지 등이 있습니다. XDR은 우수한 엔드포인트 보호, 더욱 강력한 분석, 더 빠른 대응 역량을 제공함으로써 보안 운영 현대화의 기본적인 요소로 자리매김하고 있습니다. 특히, 평균적인 기업이 최대 45개의 보안 도구를 사용하고 있고 약 19개 도구를 조율해야 인시던트에 대응할 수 있는 상황을 고려하면 당연한 결과입니다.[13]

XDR은 알림 통합, 표준화, 상관관계를 결합하고, SOAR로 확장하여 자동 조사와 개선을 지원할 수 있습니다.

탐지와 대응의 공백을 메워주는 XDR

XDR이 등장하기 전까지 엔드포인트의 원격 분석 지표와 다른 이벤트 데이터의 상관관계를 파악하기 위해서는 SIEM에서 방대한 데이터를 일일이 선별해야 했습니다. 여러 이벤트의 상관관계를 파악하는 것은 리소스 집약적인 작업으로, 사용할 데이터 소스를 결정하고 위협을 발견하기 위한 탐지 규칙을 작성하는 과정에서 숙련된 애널리스트의 지원이 필요합니다. 따라서 SOC 팀은 데이터를 수동으로 분석하고, 규칙을 작성하고, 이후 모든 알림의 정확성을 확인하는 데 막대한 시간을 소비하게 됩니다. 그 결과 언제든지 침해로 이어질 수 있는 실제 공격을 조사할 시간이 부족해집니다.

엔드포인트의 관점에서 위협을 살피는 것만으로는 충분하지 않습니다. 조직은 AI 및 분석 기반의 단일 정보 출처를 통해 엔드포인트와 클라우드, 네트워크 데이터를 통합해야 합니다.

이런 끝없는 보안 '두더지 잡기'에 속도가 저하되고 공격의 정교함과 빈도가 늘어남에 따라, 미래 지향적인 보안 조직은 보안 아키텍처에 적용한 XDR 접근 방식에서 얻은 효율성을 최대한 활용하고 있습니다. 이러한 조직들은 수동으로 며칠씩 걸리던 평균 탐지 시간(MTTD)이 AI 기반 분석을 통해 실시간으로 단축되는 것을 경험하고 있습니다. 이는 주도권이 공격자에서 방어자로 넘어가고 있음을 의미합니다.

요점 정리: Cortex XDR은 다양한 형태의 SecOps 아키텍처에 유연하게 적용할 수 있으며, EDR/EPP를 기본으로 하는 예방 기능과 함께 엔터프라이즈급 위협 탐지 및 대응을 지원합니다. SOC는 XDR에서 Cortex XSIAM®으로 진화할 수 있으며, Cortex XSIAM®은 XDR, CDR, SOAR, SIEM, 공격 표면 관리 등을 하나의 AI 기반 보안 운영 플랫폼으로 통합합니다.

13. *2020 Cyber Resilient Organization Report*, IBM Security, 2020년 6월.

요점 4: 클라우드 보안 강화 - 클라우드 보안과 SOC 운영 간 격차 해소

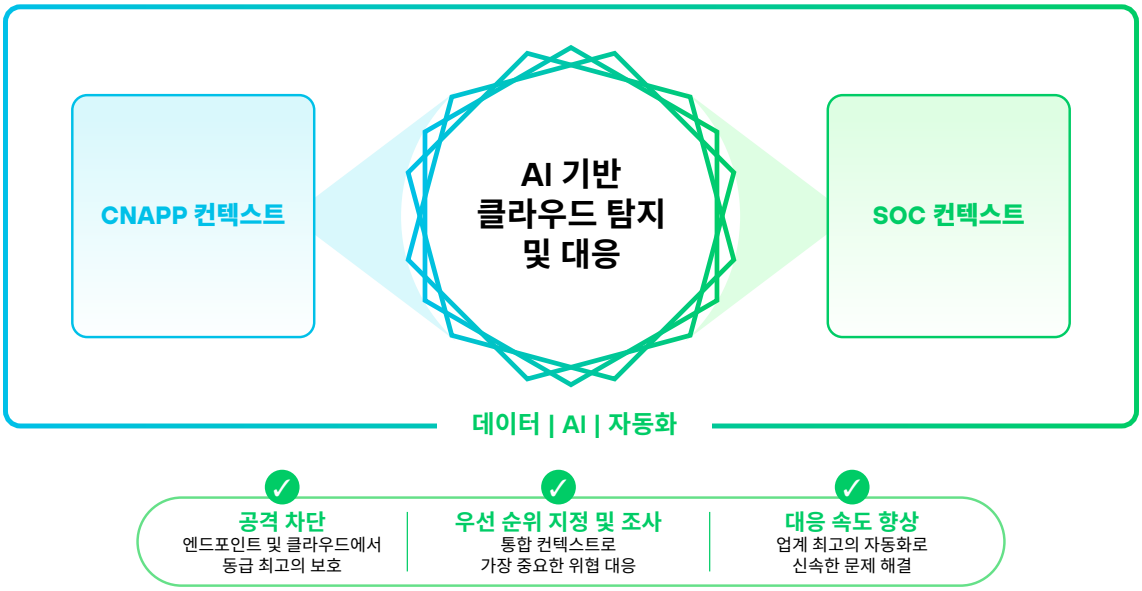

그림 5: AI 기반 CDR을 통해 클라우드 보안을 광범위한 보안 에코시스템으로 가져와 최고의 보호를 제공합니다.

오늘날의 보안팀은 사일로 방식으로 운영되는 경우가 많습니다. 클라우드 보안팀과 SecOps 팀이 서로 다른 플랫폼에서 별도의 워크플로로 작업하는 것입니다. 이러한 사일로 방식은 인시던트 대응을 지연시켜 리스크를 초래하며, 정교한 클라우드 공격에 대한 취약점을 유발합니다. 기존의 보안 도구는 클라우드 네이티브 서비스와 구성에 대한 가시성이 부족합니다. 그리고 클라우드 환경의 규모와 동적 특성에 따라 수천 개의 알림이 발생하며, 그 우선순위를 효과적으로 지정하기 어렵습니다.

일반적인 클라우드 공격 시나리오를 통해 다음과 같은 문제점을 확인할 수 있습니다. 공격자는 고객용 웹사이트를 실행하는 컨테이너의 제로데이 취약점을 악용하고, 컨테이너 이스케이프 기법을 통해 호스트 시스템으로 침입합니다. 그리고 도난당한 액세스 토큰을 사용하여 인프라를 통한 내부망 이동을 감행합니다. 기존 솔루션은 침해 지표가 데이터 사일로 곳곳에 분산되어 있어, 보안팀이 개별 지표를 감지하더라도 전체 공격을 놓치는 경우가 많습니다.

SIEM 도구는 클라우드 로그를 모니터링하지만, 데이터를 이해하기 위해서는 보안 애널리스트가 수동으로 결과를 해석하고 연관관계를 분석해야 합니다. 이 시나리오는 기존 접근 방식만으로는 부족한 이유를 분명히 보여줍니다. 런타임에서 실시간 보호가 이루어지지 않을 경우 공격자는 팀이 공격의 존재를 감지하기도 전에 클라우드 인프라를 자유롭게 이동할 수 있습니다.

클라우드 보안에서 점점 더 커져가는 주요 문제는 다음과 같습니다.

- 클라우드 워크로드가 직면하는 위협 증가(예: 컨테이너 이스케이프, 크립토마이닝, 리버스 셸 공격)
- 기존 보안 도구의 런타임 가시성 부족으로 네이티브 공격 패턴 최대 80% 누락[14]
- 지난 1년간 클라우드 공격 66% 증가[15]
- 너무 많은 도구: 포인트 제품이 늘어나며 클라우드 복잡성 증가(조직당 사용하는 클라우드 보안 도구 평균 16개 이상)[16]

14. *Unit 42 공격 표면 위협 보고서*, Palo Alto Networks, 2023년 9월 14일.
15. *2024년 Unit 42 인시던트 대응 보고서*, Palo Alto Networks, 2024년 2월 20일.
16. *클라우드 네이티브 보안 현황 보고서*, Palo Alto Networks, 2024년 2월.

Cortex® 클라우드 탐지 및 대응(CDR)은 다음과 같은 세 가지 핵심 기능으로 문제를 해결합니다.

- **런타임 예방**: MITRE ATT&CK 평가에서 100% 예방 기록을 달성한 XDR 에이전트 활용[17]
- **더 빠른 위협 탐지**: 클라우드 대상 위협에 대해 학습된 머신러닝 모델 사용, 탐지 시간 단축(몇 주 → 몇 분)
- **자동 대응**: 즉각적 대응 작업으로 신뢰성 높은 공격 시나리오에 대해 자동화된 플레이북 구현

요점 정리: Cortex CDR은 실시간 보호, AI 기반 위협 탐지, 자동 대응 기능을 제공하여 클라우드 보안 운영을 혁신합니다. 이를 통해 조직은 클라우드 환경을 보호하면서 보안팀 간의 운영 사일로를 제거할 수 있습니다.

CDR은 하이브리드 환경 전반에 걸쳐 통합적 가시성, 탐지, 자동 대응을 통해 클라우드 네이티브 보안과 SOC 운영을 결합합니다.

Cortex 플랫폼은 Cortex XDR, XSOAR, XSIAM과 통합하여 포괄적 위협 탐지, 자동 대응 조치, AI 기반 분석 기능을 제공함으로써 CDR의 기능을 강화합니다. 이러한 통합을 통해 조직은 탁월한 가시성을 확보하고 여러 보안 솔루션을 관리하는 데 따른 복잡성을 줄일 수 있습니다.

요점 5: XSIAM - 대응 속도를 높이고 위협보다 한발 앞서는 AI 기반 SOC 플랫폼

기존의 SIEM 중심 보안 운영 모델은 오늘날의 위협 환경에 적합하지 않습니다. SIEM 솔루션은 수년간 보안 운영에 활용되어 왔지만, 수동 탐지와 대응에 의존하는 방식으로는 불과 몇 시간 내에 엔드투엔드 공격을 실행하는 최신 사이버 위협에 효과적으로 대응하기 어렵습니다.

확장된 보안 인텔리전스 및 자동화 관리를 제공하는 Cortex XSIAM은 AI 우선 접근 방식을 통해 보안 운영을 혁신합니다. 핵심 보안 기능을 단일 플랫폼으로 통합합니다.

- 단일 SOC UI로 SOC 분석가 작업 간소화 및 가속화
- 전체 컨텍스트에 기반한 분석을 통해 데이터 사일로 제거
- AI 기반 방어로 위협 차단 시간을 며칠에서 몇 분 단위로 단축
- SOC 워크플로 가속화를 위한 자동 운영

XSIAM의 효과는 Palo Alto Networks의 자체 SOC를 통해 입증되었습니다. 이 SOC는 매달 1조 건 이상의 이벤트를 처리하며, 사람의 대응이 필요한 핵심 인시던트만을 표면화합니다. XSIAM은 SIEM, EDR, XDR, SOAR, CDR, ASM, UEBA, TIP 등 동급 최고의 보안 운영 기능을 모두 통합합니다. XSIAM은 모든 보안 데이터를 중앙 집중화하고, 보안을 위해 특별히 설계된 AI 모델을 사용합니다. 이를 통해 데이터 통합, 분석 및 대응 조치를 자동화하면 애널리스트가 중요한 인시던트에 집중할 수 있습니다.

요점 정리: XSIAM은 인간 중심의 보안 운영에서 AI 중심의 보안 운영으로의 전환을 의미합니다. 여러 보안 기능을 통합하고 반복 작업을 자동화함으로써 위협 탐지 및 대응 능력을 획기적으로 향상시키는 동시에 비용과 복잡성을 줄일 수 있습니다. 프로덕션 환경에서 입증된 플랫폼의 성공은 AI 시대에 적합한 보안 운영 체계로의 혁신을 뒷받침합니다.

Cortex 제품군

솔직히 말해, 대부분 고객과 잠재적 고객은 시스템 통합업체가 되는 것을 원하지 않고 반복적인 수동 작업도 달가워하지 않습니다. 사일로화된 도구가 많으면 유지에 엄청난 시간과 비용이 소요됩니다. 이질적 솔루션이 많으면 복잡성이 심해지고 가시성이 떨어져 최신 SOC에 필요한 분석에 차질을 빚기 때문에, 보안 성과가 떨어질 수 있습니다.

17. *MITRE ATT&CK Enterprise 2024 Evaluations*, MITRE, 2024년 12월.

하루에 주어진 시간을 늘릴 수는 없어도, 고객이 최적화를 수행하고 TCO를 절감하며, 다른 어느 보안 제공업체보다도 많은 타사 도구와의 통합을 지원해 운영을 한 단계 업그레이드하도록 도울 수는 있습니다. 이러한 결과뿐만 아니라 보안 애널리스트가 데이터를 안전하게 지키는 도구를 제공해 일상적인 업무에 들이는 시간을 줄이고 중요한 업무에 주력하도록 지원할 수 있다는 것도 장점입니다.

Cortex 제품군을 배포하면 SOC 여정을 시작하거나 진행 속도를 높일 수 있습니다. Cortex XSIAM , Cortex XDR, Cortex XSOAR® 및 Cortex Xpanse는 보안 운영에서 상호 보완하며 원활하게 작동합니다. 즉각적인 장점을 간략하게 소개하면 다음과 같습니다.

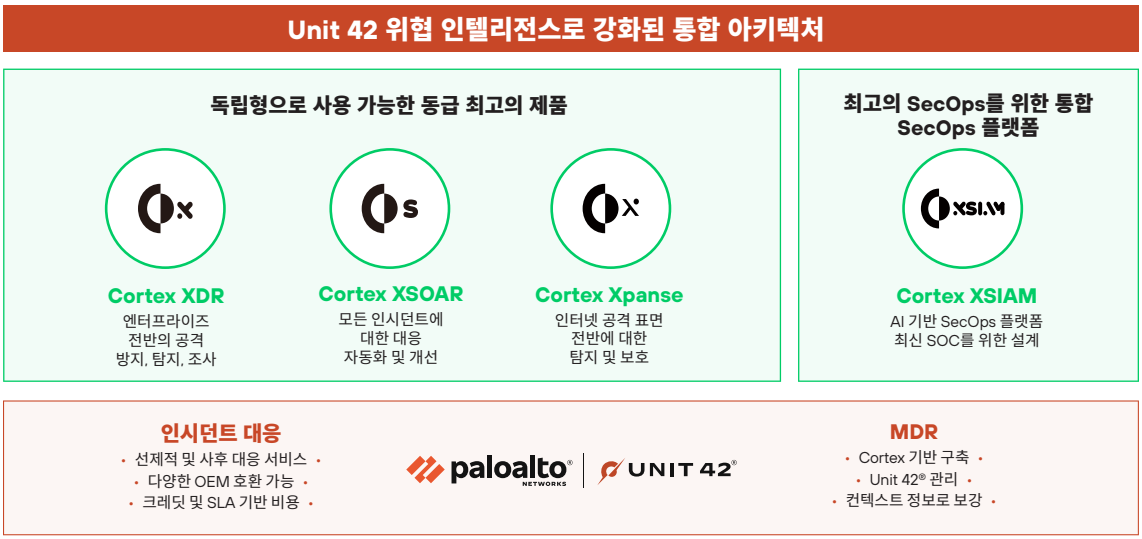

그림 6: Cortex 솔루션을 통한 유연성과 성장

Cortex 제품군은 플랫폼 접근 방식을 위한 통합 솔루션을 제공합니다.

- **Cortex Xpanse**: 인터넷에 연결된 자산과 구성 오류를 발견하고 평가하여 외부 공격 표면을 지속적으로 모니터링하고 보호합니다.
- **Cortex XSOAR**: 900개 이상의 통합 팩으로 인시던트를 관리하는 단일 플랫폼으로, 보안 워크플로를 오케스트레이션하고 위협 인텔리전스를 자동화합니다.
- **Cortex XDR**: Windows 및 Linux 환경에 세계 최고 수준의 EDR을 제공하며, 증거 수집 및 조사 과정을 자동화함으로써 모든 분석가의 신속한 대응을 지원합니다.
- **Cortex CDR**: Cortex XDR, XSOAR, XSIAM과 통합하여 포괄적 위협 탐지, 자동 대응 조치, AI 기반 분석 기능을 제공합니다.
- **Cortex XSIAM**: SIEM, EDR, XDR, SOAR, 그리고 그 외 보안 기능을 하나의 플랫폼으로 통합하여 SOC 운영을 혁신하는 AI 기반 플랫폼입니다. 분석과 대응을 자동화하여 애널리스트가 중요한 인시던트에 집중할 수 있도록 뒷받침합니다.

Cortex와 함께 더 적은 노력으로 더 강력한 보안을 구현하는 방법을 살펴보세요.

자세한 정보는 당사 제품 페이지를 참조하세요.

Cortex Xpanse | Cortex XSOAR | Cortex XDR | Cortex CDR | Cortex XSIAM

데모를 예약하고 싶으신가요? 지금 시작하세요.

paloalto NETWORKS

서울특별시 서초구 서초대로74길 4,
1층 (삼성생명 서초타워)

Tel: +82-2-568-4353
eMail: Sales-KR@paloaltonetworks.com
www.paloaltonetworks.co.kr

cortex_ds_how-to-plan-for-tomorrows-soc-today_040125